Quantifying Measurement Incompatibility of Mutually Unbiased Bases

Sébastien Designolle,[1] Paul Skrzypczyk,[2] Florian Fröwis,[1] and Nicolas Brunner[1]
[1]Département de Physique Appliquée, Université de Genève, 1211 Genève, Switzerland
[2]H.H. Wills Physics Laboratory, University of Bristol, Tyndall Avenue, Bristol BS8 1TL, United Kingdom

(Received 29 May 2018; published 6 February 2019)

Quantum measurements based on mutually unbiased bases are commonly used in quantum information processing, as they are generally viewed as being maximally incompatible and complementary. Here we quantify precisely the degree of incompatibility of mutually unbiased bases (MUB) using the notion of noise robustness. Specifically, for sets of k MUB in dimension d, we provide upper and lower bounds on this quantity. Notably, we get a tight bound in several cases, in particular for complete sets of $k = d + 1$ MUB (using the standard construction for d being a prime power). On the way, we also derive a general upper bound on the noise robustness for an arbitrary set of quantum measurements. Moreover, we prove the existence of sets of k MUB that are operationally inequivalent, as they feature different noise robustness, and we provide a lower bound on the number of such inequivalent sets up to dimension 32. Finally, we discuss applications of our results for Einstein-Podolsky-Rosen steering.

DOI: 10.1103/PhysRevLett.122.050402

Introduction.—Contrary to classical physics, different measurements in quantum mechanics can be incompatible, meaning that one cannot have access to their results simultaneously. Incompatible measurements thus provide complementary information about a quantum system. Motivated by the question of finding the measurements that are "maximally incompatible," Schwinger and others [1–4] discussed the concept of mutually unbiased (bases) measurements.

Formally, in a complex Hilbert space of dimension d, two orthonormal bases $\{|\varphi_a\rangle\}_{a=1,\ldots,d}$ and $\{|\psi_b\rangle\}_{b=1,\ldots,d}$ are called *mutually unbiased* if

$$|\langle\varphi_a|\psi_b\rangle| = \frac{1}{\sqrt{d}} \tag{1}$$

for all a and b. That is, if a system is prepared in any eigenstate of one of the bases, then performing a measurement in the other basis gives a uniformly random outcome. These bases can thus be considered "maximally noncommutative" and "complementary" [1].

It is then natural to look for sets of k measurements, such that all pairs are mutually unbiased [2]. In the simplest case of qubits ($d = 2$), there are three mutually unbiased bases (MUB) that are given by the eigenstates of the three Pauli observables. In arbitrary dimension d, however, the construction of MUB is a difficult task. It is proven that $k \leq d + 1$ [5], and an explicit construction of complete sets of $k = d + 1$ MUB is only known when the dimension is a power of a prime, i.e., $d = p^r$ with p prime and r positive integer [4]. A long-standing open problem is to determine the maximal number of MUB in the case $d = 6$, which is conjectured to be $k = 3$ [6,7].

More generally, MUB play a central role in quantum information processing [8], and have been used in a wide range of applications such as quantum tomography [2,4], uncertainty relations [3,9,10], quantum key distribution [11,12], quantum error correction [13], as well as for witnessing entanglement [14–19] and more general forms of quantum correlations [20–22]. MUB also have strong links to other mathematical structures [23] such as finite projective planes [24,25] or orthogonal Latin squares [26].

Given the general significance of MUB, it is important to characterize their properties. While MUB represent intuitively the most incompatible quantum measurements, the goal of the present work is to precisely quantify the degree of incompatibility of arbitrary sets of MUB. As a measure of incompatibility we determine the noise robustness [27–30], namely, the minimal amount of white noise required to make a given set of k MUB in dimension d jointly measurable [31–37], i.e., compatible. We derive upper and lower bounds on this quantity for any k and d. Notably, we obtain tight bounds in many cases, in particular, for $k = d$ and $k = d + 1$ by using the standard construction of Ref. [4] when d is a prime power. On the way, we also derive a general upper bound on the noise robustness for an arbitrary set of quantum measurements.

Moreover, these results highlight some interesting properties of MUB. In particular, we find that there exist operationally inequivalent sets of MUB, in the sense that they feature a different noise robustness. Lower bounds on the number of inequivalent sets are obtained for $k \leq 8$ and $d \leq 32$. In fact, we observe that this phenomenon becomes generic in high dimensions. Finally, our results also have direct implications for Einstein-Podolsky-Rosen steering [38]. Exploiting the strong connection existing between

joint measurability and steering [39–41], we characterize the noise robustness of a broad class of entangled states in steering experiments.

Preliminaries.—We consider sets of general quantum measurements, i.e., positive operator valued measures (POVMs). A POVM is a collection of positive-semidefinite operators summing up to identity; given a state ρ and a POVM $\{A_a\}_a$, the probability of getting outcome a is then $p(a) = \mathrm{tr}A_a\rho$. Our main focus will be to determine whether sets of POVMs (mostly noisy MUB) are compatible or not. Note that the usual notion of commutativity, used for the case of projective measurements, is inadequate for general POVMs [42]. Instead we use the notion of joint measurability [31,32].

Specifically a set of POVMs is jointly measurable if there exists a *parent* POVM from which each POVM of the set can be recovered by taking the marginals. This implies that, for any state ρ, the statistics of all POVMs in the original set can be recovered by first measuring the parent POVM, and then classically postprocessing the result. Formally, for a set of k POVMs $\{\{A_{a|x}\}_a\}_{x=1,\ldots,k}$, joint measurability is ensured by the existence of a POVM $\{\mathcal{G}_{\vec{j}[k]}\}_{\vec{j}[k]}$ such that

$$\sum_{\substack{j_1,\ldots,j_{x-1}\\ j_{x+1},\ldots,j_k}} \mathcal{G}_{j_1,\ldots,j_{x-1},a,j_{x+1},\ldots,j_k} = \sum_{\vec{j}[k]} \delta_{j_x,a}\mathcal{G}_{\vec{j}[k]} = A_{a|x}. \quad (2)$$

Here and in the following, the notation $\vec{j}[k]$, often abbreviated $\vec{j}$ if k is clear in the context, means $j_1, \ldots, j_k$.

Beyond this dichotomy of compatible vs incompatible, it is interesting to *quantify* how incompatible a set of POVMs is. A general way to do so consists in mixing each POVM of the set with white noise. This defines a new set of noisy POVMs, where each POVM element is given by

$$A^{\eta}_{a|x} = \eta A_{a|x} + (1-\eta)\mathrm{tr}A_{a|x}\frac{\mathbb{1}}{d}. \quad (3)$$

Physically, for rank-one projective measurements, this amounts to performing the measurement $A_{a|x}$ with probability η, and outputting at random with probability $1-\eta$. By adding more and more noise to a set of incompatible POVMs, it is intuitive that it will eventually become jointly measurable. Indeed, when $\eta = 0$, only white noise remains so that joint measurability is ensured. The critical parameter η^* at which the transition occurs is the noise robustness, a meaningful incompatibility quantifier [27,29,30].

General upper bound.—First we consider a general set of k POVMs $\{\{A_{a|x}\}_a\}_x$. Its noise robustness η^* can be expressed as the following semidefinite program (SDP) [27]; see also Ref. [43].

$$\begin{aligned} \eta^* = \max_{\eta,\{\mathcal{G}_{\vec{j}}\}_{\vec{j}}} \quad & \eta \\ \text{s.t.} \quad & \sum_{\vec{j}} \delta_{j_x,a}\mathcal{G}_{\vec{j}} = A^{\eta}_{a|x} \quad \forall\ a,x, \\ & \mathcal{G}_{\vec{j}} \geq 0 \quad \forall\ \vec{j}, \quad \eta \leq 1. \end{aligned} \quad (4)$$

This formulation is well known and has already been studied *numerically*, even with MUB [44]. Nonetheless, since we want *analytical* results, we make use of a powerful tool used to study SDP, namely, duality theory. Every SDP admits a dual program whose solution is greater than (weak duality) or equal to (strong duality) the primal one [45]. In our case, the dual formulation of Eq. (4) is

$$\begin{aligned} \eta^* = \min_{\{X_{a|x}\}_{a,x}} \quad & 1 + \mathrm{tr}\sum_{a,x} X_{a|x}A_{a|x} \\ \text{s.t.} \quad & 1 + \mathrm{tr}\sum_{a,x} X_{a|x}A_{a|x} \geq \frac{1}{d}\sum_{a,x}\mathrm{tr}A_{a|x}\mathrm{tr}X_{a|x}, \\ & \sum_{a,x}\delta_{j_x,a}X_{a|x} \geq 0 \quad \forall\ \vec{j}, \end{aligned} \quad (5)$$

where $X_{a|x}$ are new (dual) variables. The equality with η^* is ensured since strong duality holds in our case (see Sec. I of Supplemental Material [46] for details).

Importantly, from Eq. (5) it is then clear that the value of $1 + \mathrm{tr}\sum_{a,x} X_{a|x}A_{a|x}$ corresponding to any $\{X_{a|x}\}_{a,x}$ that satisfies the constraints is an upper bound to η^*. In Sec. I of Supplemental Material [46], we show that the following variables satisfy and saturate the constraints

$$X_{a|x} = \frac{\frac{\lambda}{k}\mathbb{1} - A_{a|x}}{\sum_{a',x'}\left[\mathrm{tr}A^2_{a'|x'} - \frac{1}{d}(\mathrm{tr}A_{a'|x'})^2\right]}, \quad (6)$$

where

$$\lambda = \max_{\vec{j}} \|S_{\vec{j}}\|_\infty \quad \text{and} \quad S_{\vec{j}} = \sum_{x=1}^{k} A_{j_x|x}. \quad (7)$$

This gives rise to the following bound on the noise robustness

$$\eta^* \leq \frac{\lambda - \sum_{a,x}\left(\frac{\mathrm{tr}A_{a|x}}{d}\right)^2}{\sum_{a,x}\left[\frac{\mathrm{tr}A^2_{a|x}}{d} - \left(\frac{\mathrm{tr}A_{a|x}}{d}\right)^2\right]} = \eta_{\mathrm{up}}. \quad (8)$$

When $\{\{A_{a|x}\}_a\}_x$ are rank-one projective measurements, this further simplifies to

$$\eta_{\mathrm{up}} = \frac{\lambda - \frac{k}{d}}{k - \frac{k}{d}}. \quad (9)$$

Upper bound for MUB.—Notably, the bound (9) is also valid for projective measurements on k MUB. Since there are d^k (i.e., exponentially many) operators $S_{\vec{j}}$ to check in the definition (7) of λ, this becomes computationally intractable very quickly. A way to get a quick estimate of η_{up} is to use a bound on the norm of sums of projectors from Ref. [20]. In our case, thanks to the relation (1), we get $\lambda \leq 1 + (k-1)/\sqrt{d}$ which gives

$$\eta_{\mathrm{up}} \leq \frac{\frac{\sqrt{d}}{k}+1}{\sqrt{d}+1}. \tag{10}$$

This simple expression is, however, rarely tight.

Note that to derive the bound (10), the only assumption used is the unbiasedness (1). Later, we also derive a lower bound based only on this hypothesis. However, in general, this alone is not sufficient to fix the value of η^*. Indeed, as we will show below, inequivalent sets of MUB can have different η^*. Thus to go further than only bounding η^*, we will use explicit sets of MUB.

Tightness for specific MUB.—Here we exploit a specific implementation of MUB to analytically and numerically investigate the behavior of the noise robustness η^* and the performance of the upper bound η_{up}. Since the construction of complete sets of MUB in prime power dimensions by Wootters and Fields [4] was reformulated in many equivalent ways [8,47–49], we choose different implementations depending on our needs. We use the construction of Ref. [8] for numerical purposes since it is easy to implement, and the one of Ref. [48] when it comes to analytical results taking advantage of the properties of the underlying algebraic structures [50–52].

Table I presents the solution η^* of the SDP (5) together with the upper bound η_{up} defined in Eq. (9) for low dimensions $d \leq 7$. In some cases (e.g., triplets in dimension five and quadruplets in dimension seven), two solutions were obtained depending on the choice of the subset of MUB. We discuss these inequivalent sets in more detail below.

Notice that the equality $\eta^* = \eta_{\mathrm{up}}$ holds in a number of cases (bold font). In particular, when $k = 2$, $k = d$, and $k = d + 1$, we prove this tightness analytically by providing an explicit parent POVM for $\{A^{\eta^*}_{a|1}\}_a, \ldots, \{A^{\eta^*}_{a|k}\}_a$. It is given by the operators

$$\mathcal{G}_{\vec{j}} = \begin{cases} \Pi_{\vec{j}} & \text{if } \|S_{\vec{j}}\|_\infty = \lambda \\ 0 & \text{otherwise,} \end{cases} \tag{11}$$

where $\Pi_{\vec{j}}$ is the projector on the eigenspace of $S_{\vec{j}}$ associated with the maximum eigenvalue, which is λ in that case.

For $k = 2$, this was already known [36,37] and the above parent POVM indeed coincides with the one proposed in Sec. IV of Ref. [37].

For $k = d$ and $k = d + 1$, the proof of validity and optimality of this parent POVM (11) is more involved and consists of the following steps. (i) From Sec. I of Supplemental Material [46] we know that, as soon as $\mathcal{G}_{\vec{j}}$ is a parent POVM for noisy MUB, our upper bound is tight. (ii) We express $\mathcal{G}_{\vec{j}}$ as $\lim_{n\to\infty}\mathcal{G}^{(n)}_{\vec{j}}$ where $\mathcal{G}^{(n)}_{\vec{j}} = (S_{\vec{j}}/\lambda)^n$. (iii) We prove the normalization of the $\mathcal{G}^{(n)}_{\vec{j}}$, namely, $\sum_{\vec{j}}\mathcal{G}^{(n)}_{\vec{j}} \propto \mathbb{1}$, from which the normalization of $\mathcal{G}_{\vec{j}}$ is set. (iv) We compute the marginals of $\mathcal{G}^{(n)}_{\vec{j}}$. This step is the only one in which the assumption $k = d$ or $k = d + 1$ is used. The complete proof can be found in Sec. IV of Supplemental Material [46].

We stress that, although the proof gives a fully analytical result—in the sense that the noise robustness η^* is formally an eigenvalue of a specific operator—actually solving analytically this eigenvalue problem leads to the resolution of a polynomial equation whose explicit solution does not exist in general. Apart from the case of two MUB in any dimension [37], the cases in which we found such an explicit form are listed in Sec. III of Supplemental Material [46]. Additionally, there are special cases in which the upper bound is also reached. This can be seen numerically either by comparing the result η^* of the SDP (5) with the value of η_{up} or by checking that the operators defined in Eq. (11) form a parent POVM for $\{A^{\eta^*}_{a|1}\}_a, \ldots, \{A^{\eta^*}_{a|k}\}_a$ (see Sec. III of Supplemental Material [46]).

TABLE I. Noise robustness η^* of sets of k MUB in dimension $d \leq 7$. For each case, we give the exact or approached values of η^* and the upper bound η_{up}. Instances for which the bound is tight, i.e., $\eta^* = \eta_{\mathrm{up}}$, are indicated by bold fonts, in particular, $k = 2$, $k = d$, and $k = d + 1$. Moreover, this shows the existence of operationally inequivalent sets of MUB, featuring different values of η^*. For instance, there are two inequivalent quadruplets for $d = 7$, and $\eta^* = \eta_{\mathrm{up}}$ holds for one of them. For $d = 6$ only three MUB could be constructed so far, but a bound could still be derived for $k = 4$ (see Sec. II of Supplemental Material [46]).

k	d									
	2	3	4		5		6		7	
	$\eta^* = \eta_{\mathrm{up}}$	$\eta^* = \eta_{\mathrm{up}}$	η^*	η_{up}	η^*	η_{up}	η^*	η_{up}	η^*	η_{up}
2	$\mathbf{1/\sqrt{2} \approx 0.7071}$	$\mathbf{[(1+\sqrt{3})/4] \approx 0.6830}$	$\mathbf{\frac{2}{3} \approx 0.6667}$		$\mathbf{[(3+\sqrt{5})/8] \approx 0.6545}$		$\mathbf{[(4+\sqrt{6})/10] \approx 0.6449}$		$\mathbf{[(5+\sqrt{7})/12] \approx 0.6371}$	
3	$\mathbf{1/\sqrt{3} \approx 0.5774}$	$\mathbf{\{[\cos(\pi/18)]/\sqrt{3}\} \approx 0.5686}$	0.5469	0.5556	$\mathbf{[(1+\sqrt{5})/6] \approx 0.5393}$ $\mathbf{\{[13-\sqrt{5}+\sqrt{30(5+\sqrt{5})}]/48\} \approx 0.5312}$		0.5204	0.5254	0.5101	0.5154
4		$\mathbf{[(1+3\sqrt{5})/16] \approx 0.4818}$	$\mathbf{\frac{1}{2} = 0.5000}$		0.4615	0.4616	?	≤ 0.4550	**0.4516**	
									0.4436	0.4488
5			$\mathbf{[(3+2\sqrt{3})/15] \approx 0.4309}$		**0.4179**		?		0.4049	0.4120
6					**0.3863**		?		0.3754	0.3867
7							?		**0.3685**	
8									**0.3318**	

Inequivalent sets of MUB.—When constructing sets of k MUB in dimension d, there is some freedom. In fact, it is known that (for certain k and d) there exist sets of MUB that are inequivalent under unitaries, overall complex conjugation, and other trivial operations like permutations or phase shifts [53]. In the following we will simply refer to such sets as *inequivalent*.

Here, we go one step further, and show that there are sets of MUB that are operationally inequivalent, in the sense that they feature different values of η^*. For instance, this is the case for $k=3$ and $d=5$, where there are two inequivalent sets (see Table I). From the definition (5), it is clear that operationally inequivalent sets are necessarily inequivalent. However, the converse does not hold as proven, e.g., by pairs of MUB in dimension four [53]. Note that in practice computing η^* becomes quickly demanding. Nevertheless we can obtain lower bounds on the number of sets featuring a different value of the upper bound η_{up}. In turn, this gives a lower bound on the number of inequivalent sets; indeed equivalent sets give the same η_{up} [see Eq. (9)]. In Table II we give lower bounds on the number of inequivalent sets of MUB. Interestingly, inequivalent sets seem to become more and more frequent in high dimension (except when d is a power of two).

Lower bound for MUB.—Here we construct a very general parent POVM for noisy MUB using only the mutual unbiasedness (1) of the bases. It is a generalization of the construction presented in Ref. [37] for two MUB.

Let $|\chi^1_{\vec{j}}\rangle$ be defined iteratively by $|\chi^1_{j_1}\rangle = |\varphi^1_{j_1}\rangle$, the j_1th vector of the first basis, and

$$|\chi^1_{\vec{j}[k]}\rangle = (\mathbb{1} + \alpha_k \sqrt{d} A_{j_k|k})|\chi^1_{\vec{j}[k-1]}\rangle, \tag{12}$$

where α_i are positive coefficients introduced for later optimization. Now let $|\chi^y_{\vec{j}}\rangle$ be defined similarly but with basis indices circularly shifted according to $y = 1, \ldots, k$. Specifically, $|\chi^y_{j_1}\rangle = |\varphi^y_{j_1}\rangle$, the j_1th vector of the yth basis, and, in the exponents of Eq. (12), 1 becomes y, 2 becomes $y+1$ (modulo k), etc. Now a straightforward iterative proof shows that

$$\mathcal{G}_{\vec{j}[k]} = \sum_{y=1}^{k} |\chi^y_{\vec{j}[k]}\rangle\langle\chi^y_{\vec{j}[k]}| \tag{13}$$

is, up to normalization, a parent POVM for $\{A^{\eta_k}_{a|1}\}_a, \ldots, \{A^{\eta_k}_{a|k}\}_a$, where η_k is defined recursively by $\eta_1 = 1$ and

$$\eta_k = \frac{(2\alpha_k\sqrt{d} + d)(k-1)\eta_{k-1} + (2\alpha_k\sqrt{d} + \alpha_k^2 d)}{k(2\alpha_k\sqrt{d} + (\alpha_k^2 + 1)d)}. \tag{14}$$

Then we can optimize over the coefficients $\alpha_2, \ldots, \alpha_k$ to get the highest possible noise parameter (see Sec. V of Supplemental Material [46] for details). The best value achieved is denoted η_{low}. Since an explicit parent POVM of k MUB with a noise parameter η_{low} was constructed, the noise robustness η^* is indeed greater than η_{low}. While these bounds are only tight when $k=2$ or $d=2$, they are straightforward to compute and quite insightful. For $d \leq 7$, its approximated values are given in Sec. V of Supplemental Material [46].

Implications for EPR steering.—Our results also have implications for EPR steering, due to the intimate relation that exists with joint measurability [39–41]. Specifically, our bounds on η^* imply bounds on the noise robustness of certain entangled states for demonstrating steering. Consider quantum states of the form

$$\rho^w_\psi = w|\psi\rangle\langle\psi| + (1-w)\mathbb{1}/d \otimes \text{tr}_A|\psi\rangle\langle\psi|, \tag{15}$$

where $|\psi\rangle$ is an arbitrary pure entangled state of dimension $d \times d$. It is interesting to determine the critical noise robustness w^*, i.e., the smallest value of w such that ρ^w demonstrates steering from the first party (Alice) to the second (Bob). In general, w^* depends on the set of measurements performed by Alice. In the case she performs k (noiseless) MUB measurements, we have that $w^* = \eta^*$, and hence all our results apply directly. In the general case where Alice can perform all possible measurements, then we get the upper bound $w^* \leq \eta^*$. We refer to Sec. VI of Supplemental Material [46] for details.

Conclusion.—We discussed the problem of quantifying the measurement incompatibility of MUB. We derived bounds on the noise robustness, which turn out to be tight in many cases, in particular for the standard construction of complete sets of $k = d+1$ MUB [4]. While our proof does not apply directly to other constructions of complete sets of MUB, we nevertheless conjecture that our bound is tight for any construction. We could check this numerically for another inequivalent construction in dimension $d=8$ [54]. We also provided a general upper bound on the noise robustness for any set of POVMs. It would be interesting to see how this bound performs for measurements that are not

TABLE II. Lower bound on the number of inequivalent sets of MUB. Bold letter fonts indicate operationally inequivalent sets (different values of η^*). When k is greater than the number of MUB constructed in Ref. [4], the cell is left empty. Dimensions for which no inequivalent sets were found are not presented (e.g., dimensions 4, 6, 8, 32).

k	d																	
	5	7	9	11	13	15	16	17	19	20	21	23	25	27	28	29	31
3	**2**	**1**	**2**	**1**	**2**	**2**	**1**	2	1	2	2	1	2	1	1	2	1
4	**1**	**2**	**3**	**2**	**4**	**1**	1	4	4	1	1	4	3	2	2	6	6
5	**1**	**1**	**3**	2	5		1	8	5	1		6	6	2	1	19	11
6	**1**	**1**	3	4	7		1	15	13			22	9	6		67	50
7		**1**	2	2	10		1	20	18			32	38	9		145	92
8		**1**	1	2	7		2	23	22			35	?	?		?	?

MUB, and whether one could find analytical solutions in other cases.

We showed the existence of operationally inequivalent sets of MUB, and provided lower bounds on their number. We observed that inequivalent sets become more and more frequent in high dimensions. Whether there exist operationally inequivalent sets of $k = d + 1$ MUB remains a problem to be addressed.

Finally, our results have direct implications for EPR steering. An interesting open question is whether complete sets of $d + 1$ MUB are the most robust among all sets of $d + 1$ measurements, as conjectured in Ref. [44]. In Sec. VII of Supplemental Material [46], we give further support for this conjecture by proving it, in particular, for qubit projective measurements [55]. For general qubit measurements as well as for higher dimensions, this question is left open.

Financial support by the Swiss National Science Foundation No. 172590 (Starting Grant DIAQ, NCCR-QSIT), the Royal Society (URF UHQT), and European ERC-AG MEC is gratefully acknowledged.

[1] J. Schwinger, Proc. Natl. Acad. Sci. U.S.A. **46**, 570 (1960).
[2] I. D. Ivanovic, J. Phys. A **14**, 3241 (1981).
[3] K. Kraus, Phys. Rev. D **35**, 3070 (1987).
[4] W. K. Wootters and B. D. Fields, Ann. Phys. (N.Y.) **191**, 363 (1989).
[5] I. Bengtsson, AIP Conf. Proc. **889**, 40 (2007).
[6] S. Brierley and S. Weigert, Phys. Rev. A **78**, 042312 (2008).
[7] P. Jaming, M. Matolcsi, and P. Mora, Crypt. Comm. **2**, 211 (2010).
[8] T. Durt, B. G. Englert, I. Bengtsson, and K. Życzkowski, Int. J. Quantum. Inform. **08**, 535 (2010).
[9] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).
[10] M. A. Ballester and S. Wehner, Phys. Rev. A **75**, 022319 (2007).
[11] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[12] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **67**, 062310 (2003).
[13] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett. **78**, 405 (1997).
[14] Y. Huang, Phys. Rev. A **82**, 012335 (2010).
[15] C. Spengler, M. Huber, S. Brierley, T. Adaktylos, and B. C. Hiesmayr, Phys. Rev. A **86**, 022311 (2012).
[16] L. Maccone, D. Bruss, and C. Macchiavello, Phys. Rev. Lett. **114**, 130401 (2015).
[17] E. C. Paul, D. S. Tasca, L. Rudnicki, and S. P. Walborn, Phys. Rev. A **94**, 012303 (2016).
[18] J. Rehacek, Z. Hradil, A. B. Klimov, G. Leuchs, and L. L. Sanchez-Soto, Phys. Rev. A **88**, 052110 (2013).
[19] P. Erker, M. Krenn, and M. Huber, Quantum **1**, 22 (2017).
[20] P. Skrzypczyk and D. Cavalcanti, Phys. Rev. A **92**, 022354 (2015).
[21] D. Sauerwein, C. Macchiavello, L. Maccone, and B. Kraus, Phys. Rev. A **95**, 042315 (2017).
[22] A. C. S. Costa, R. Uola, and O. Gühne, Phys. Rev. A **98**, 050104 (2018).
[23] M. Planat, H. Rosu, S. Perrine, and M. Saniga, Found. Phys. **36**, 1662 (2006).
[24] M. Saniga, M. Planat, and H. Rosu, J. Opt. B **6**, L19 (2004).
[25] J. L. Hall and A. Rao, International Symposium on Information Theory and its Applications, Auckland, New Zealand, 2008 (IEEE, 2008).
[26] T. Paterek, B. Dakić, and Č. Brukner, Phys. Rev. A **79**, 012109 (2009).
[27] T. Heinosaari, J. Kiukas, and D. Reitzner, Phys. Rev. A **92**, 022115 (2015).
[28] E. Haapasalo, J. Phys. A **48**, 255303 (2015).
[29] D. Cavalcanti and P. Skrzypczyk, Phys. Rev. A **93**, 052112 (2016).
[30] D. Cavalcanti and P. Skrzypczyk, Rep. Prog. Phys. **80**, 024001 (2017).
[31] P. Busch, P. Lahti, and P. Mittelstaedt, *The Quantum Theory of Measurement*, in Lecture Notes in Physics Monographs Vol. 2 (Springer, Berlin, Heidelberg, 1996).
[32] T. Heinosaari, T. Miyadera, and M. Ziman, J. Phys. A **49**, 123001 (2016).
[33] P. Busch and H. J. Schmidt, Quantum Inf. Process. **9**, 143 (2010).
[34] S. Yu, N. L. Liu, L. Li, and C. H. Oh, Phys. Rev. A **81**, 062116 (2010).
[35] R. Pal and S. Ghosh, J. Phys. A **44**, 485303 (2011).
[36] C. Carmeli, T. Heinosaari, and A. Toigo, Phys. Rev. A **85**, 012109 (2012).
[37] R. Uola, K. Luoma, T. Moroder, and T. Heinosaari, Phys. Rev. A **94**, 022109 (2016).
[38] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007).
[39] M. T. Quintino, T. Vértesi, and N. Brunner, Phys. Rev. Lett. **113**, 160402 (2014).
[40] R. Uola, T. Moroder, and O. Gühne, Phys. Rev. Lett. **113**, 160403 (2014).
[41] R. Uola, C. Budroni, O. Gühne, and J. P. Pellonpää, Phys. Rev. Lett. **115**, 230402 (2015).
[42] P. Kruszynski and W. M. de Muynch, Math. Phys. Appl. Math. **28**, 1761 (1987).
[43] M. M. Wolf, D. Perez-Garcia, and C. Fernandez, Phys. Rev. Lett. **103**, 230402 (2009).
[44] J. Bavaresco, M. T. Quintino, L. Guerini, T. O. Maciel, D. Cavalcanti, and M. T. Cunha, Phys. Rev. A **96**, 022110 (2017).
[45] S. Boyd and L. Vandenberge, *Convex Optimization* (Cambridge University Press, Cambridge, England, 2004).
[46] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.122.050402 for a detailed derivation of all the results presented in this Letter.
[47] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan, Algorithmica **34**, 512 (2002).
[48] A. Klappenecker and M. Roetteler, Lecture Notes in Computer Science, in *Proceedings of the 7th International Conference on Finite Fields (Fq7), Toulouse, France* (Springer, Berlin, Heidelberg, 2004), pp. 137–144.
[49] C. Godsil and A. Roy, Eur. J. Combinatorics **30**, 246 (2009).
[50] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Application* (Cambridge University Press, Cambridge, England, 1986), pp. 168–177.

[51] Z. X. Wan, *Finite Fields and Galois Rings* (World Scientific, Singapore, 2012).
[52] C. Carlet, One-weight Z4-linear codes, in *Coding Theory, Cryptography and Related Areas* (Springer, New York, 2000), pp. 57–72.
[53] S. Brierley, S. Weigert, and I. Bengtsson, Quantum Inf. Comput. **10**, 803 (2010).
[54] A. Sehrawat and A. B. Klimov, Phys. Rev. A **90**, 062308 (2014).
[55] S. Yu and C. H. Oh, arXiv:1312.6470.